



DEPARTMENT OF THE NAVY INTEGRATED RISK MANAGEMENT STRATEGY

ADVANCING TO A CULTURE OF EXCELLENCE



FISCAL YEARS

2020 – 2022

Version 1.0

February 2020

Table of Contents

Section	Page
Foreword	2
Executive Summary	3
Background	9
“Advancing to a Culture of Excellence”	9
Requirements	10
Why Change Now?.....	12
Current State of Risk Management and Internal Controls	13
Benefits of Integrated Risk Management	14
Vision for the Future State.....	15
How We Get There – Maturity	16
Lines of Effort	16
People	17
Processes	19
Governance	20
Technology	20
Next Steps.....	22
Appendix A. Maturity Model.....	A-1
Appendix B. References	B-1
Appendix C. Acronyms.....	C-1

List of Figures

Figure	Page
Figure 1. DON Integrated Risk Management Framework	5
Figure 2. Broadened OMB Circular No. A-123, Appendix A (2018)	6
Figure 3. DON Integrated Risk Management Maturity Model.....	6
Figure 4. PPBE Process and Impact to IRM Strategy	7
Figure 5. Risk Response Optimization.....	9
Figure 6. DON Mission and Vision Examples	10
Figure 7. Benefits of Integrated Risk Management.....	14

List of Tables

Table	Page
Table 1. Goal End-state of the DON Integrated Risk Management Maturity Model.....	17
Table 2. DON Integrated Risk Management Maturity Model.....	A-1

Foreword

Message from ASN FM&C

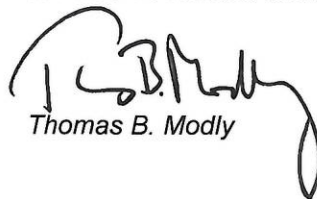
The IRM strategy establishes a framework for the DON's risk management practices to aid in the identification, prioritization, and response to enterprise risks that could hinder the DON's ability to successfully execute the National Defense Strategy (NDS). The IRM strategy provides a roadmap to enhance the efficiency, effectiveness, and transparency of both risk assessments and their associated risk response strategies (including internal controls) across the DON. This will enable us to meet mission requirements and make strides toward achieving our goal of improved and auditable business practices for greater operational readiness and affordability. DON's IRM strategy is the solution needed to meet reporting standards and improve decision making, now and in the future.



Thomas W. Harker

Message from the UNSECNAV

Over the past year, the DON has initiated several key strategies to continuously improve and better monitor the way we man, train, and equip our Navy and Marine Corps in support of the NDS and the DON's FY20-22 Business Operations Plan. Specifically, the DON has focused on education, human capital, information management and logistics supply chain modernization. A crucial piece to sustaining this progress is strengthening our "calculated risk" capabilities as we make decisions to prioritize improvement opportunities in DON business operations. The IRM maturity model approach, described in this document, outlines the foundational structure necessary to provide a streamlined and systematic approach to decision making. Additionally, it aligns the DON's enterprise-wide decision processes with the management of our major strategic focus areas and operational processes essential to achieving our Title 10 mission and goals.



Thomas B. Modly



Executive Summary

"The DON must move with a sense of urgency to improve how we manage the Department in order to continually reinvest into the improved readiness and modernization of our force. While doing so, we will create a more agile and accountable organization that not only responds rapidly and with precision, but also anticipates future threats and opportunities."

-Thomas B. Modly, UNSECNAV



In an increasingly complex and dynamic global environment, leadership decisions across the DON have a direct impact on sustained maritime superiority, readiness, and lethality. Gone are the days when management decisions could be made in a vacuum or resources wasted due to time spent on “compliance exercises” and “paper-drills” with little added value. Every minute not spent maximizing our limited resources in support of Navy and Marine Corps forces is a barrier to achieving our core mission. The purpose of this strategy is to present an integrated DON framework and maturity model for the implementation of Enterprise Risk Management (ERM) and a phased approach to an updated Internal Controls program to improve value creation and value preservation. This document applies to all leaders and managers responsible for the people, assets, and processes to recruit, train, equip, and organize to deliver combat ready Naval forces.

Achieving integrated internal control and risk management that is incorporated into the DON's broader governance, strategy, and performance is a journey that must be deliberately orchestrated and executed while also administrating accountability. The cultural and behavioral changes required of those accountable and involved needs to be tempered and encouraged over time; they need to have a chance to catch up to incremental changes in people, processes, governance, and technology before disrupting the ecosystem with even greater change.

Risk is inherent to our operations due to the rapid pace of decision-making and the decentralized nature of the DON. The DON has significant existing risk management capabilities and monitoring processes from a warfighting perspective, but less so for business operations. Many of these are specific to individual organizations, units, or functions. In the evolutionary model for risk management at the DON, these specific processes will continue to add value for their discrete purposes as the DON transitions to the new and broader IRM framework. IRM will consist of two programs: ERM and Internal Controls over Reporting (ICOR), which will work in complementary but distinct ways.

Achieving full operational capacity and integration does not happen overnight, especially for an organization with complex programs and operations such as the DON. They are achieved with distinct and concerted efforts within each of four key lines of effort in the DON's maturity. With an early focus on establishing and/or improving each of our ERM and ICOR Program areas, with a specific focus on transitioning ICOR, comes an opportunity to craft those programs from a mold that prioritizes their interconnectedness and the touchpoints among them. Improvements in each of the DON's support processes exerts a critical downrange effect on the warfighter. Thus, addressing business risks and closing control gaps improves the DON's preparedness, mission readiness and lethality.

ERM is the process of planning, organizing, leading, and controlling the activities of an agency in order to minimize the effects of risk and maximizing opportunities from a balanced portfolio perspective. Effective ERM requires the establishment of the appropriate mechanisms to share risk information from these discrete efforts, as well as, the cultural willingness to be transparent with these insights. Understandably, there is a reluctance around openly discussing how to manage risk due, in part, to skepticism around change. Historically, federal agencies have assessed and managed risks in silos, but in today's environment, risk management should be integrated across and throughout the enterprise.

Definition of Enterprise Risk Management: "ERM is an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery."

July 2016, OMB Circular A-123: Management's Responsibility for Enterprise Risk Management and Internal Control

ICOR will focus on improving the ability for management to focus on the most important data and reports necessary to effect these controls. The aim of this broader view of reporting is to reduce the burden on agencies by shifting away from low-value activities and toward actions that will support the reporting of high-quality data in support of data-driven decisions. There will still be an assessment of risks to achieving an agency's objectives (e.g., strategic, operations, reporting and compliance objectives).

Definition of Internal Controls Over Reporting: "The Green Book defines internal control as a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity are achieved. These objectives and related risks can be broadly classified into one or more of the following categories:

- Operations: Effectiveness and efficiency of operations;
- Reporting: Reliability of reporting for internal and external use; and
- Compliance: Compliance with applicable laws and regulations."

September 2014, GAO-14-704G: Standards for Internal Control in the Federal Government (Green Book)

Fortunately, the requirements and framework for implementing an effective risk management program have kept pace with the increasingly integrated operating posture promulgated by the NDS. The Office of Management and Budget (OMB) released a revision to Circular No. A-11 titled, "Preparation, Submission, and Execution of the Budget," which requires all agencies to implement ERM as appropriate for the agency mission and in accordance with agency-specific programs. Additionally, OMB Circular No. A-123, dated July 2016 and titled, "Management's Responsibility for Enterprise Risk Management and Internal Control" requires agencies to integrate their risk management framework with internal control functions.

At the center of risk management and internal controls are the integrated enterprise-wide processes, including End-to-End (E2E) business processes, which have a pervasive impact on the DON. Effective and agile risk management and internal controls programs cannot be achieved without integrating the enterprise-wide processes to achieve a fully cohesive and holistic risk management framework.

There are many benefits to having an integrated approach, including, prioritization of efforts, streamlining of processes, and meeting compliance requirements. By using a single integrated risk management framework to carry out ERM and internal control activities across the DON, we have an opportunity to focus on the activities that matter most. Figure 1 depicts the interconnectedness of the ERM and internal

control-related activities that ultimately support the annual Statement of Assurance (SOA) signed by the Secretary of the Navy (SECNAV).

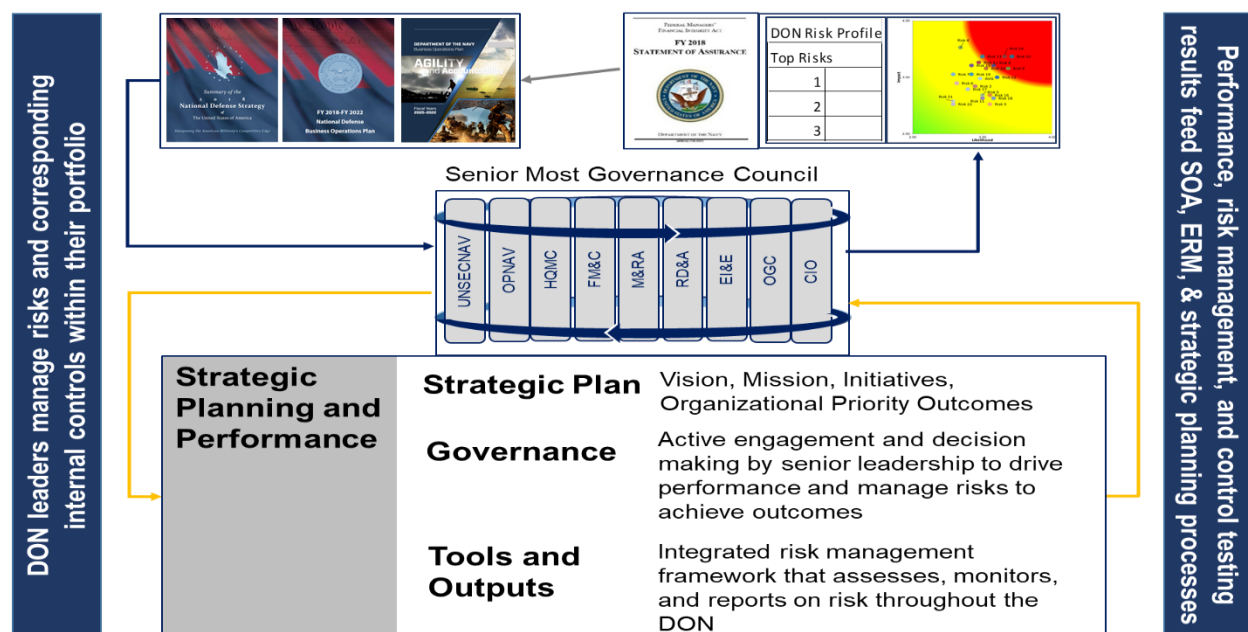


Figure 1. DON Integrated Risk Management Framework

The tenets of ERM can generate value at every level of the organization. The SECNAV and his immediate leadership team will use the insights generated through ERM to inform and enhance decision-making in pursuit of the strategic objectives of the DON. The higher-level organizational elements will further benefit from information-sharing, and integrated decision-making among the sub-enterprise functions and units to generate relevant insight as an aggregated portfolio.

In order to prepare, submit, and execute the budget, OMB Circular No. A-11 and OMB Circular No. A-123 require formal and integrated ERM and ICOR programs. IRM results in an agile, impactful, substantiated, and sustainable strategy that drives more accurate and comprehensive data processed via enterprise-wide processes, such as E2E business processes. IRM will also leverage Performance-to-Plan (P2P), an enterprise management approach that identifies performance gaps, ascertains barriers to execution, and implements solutions to improve performance. Initial efforts in P2P are focused on improving readiness outcomes. This data-driven approach helps focus leadership's attention on high leverage levers to inform a more effective allocation of resources and planning. Current key DON program and mission focus areas within P2P are Aviation (including Safety), Surface, Undersea, and Shipyards, which may expand to other areas as the IRM strategy evolves.

Planning, Programming, Budgeting and Execution (PPBE) is DoD's disciplined process to allocate resources to strategic goals. Planning establishes strategic priorities and capabilities required to achieve the strategy. Programming applies resources to programs that provide the capabilities required to achieve the strategic priorities. Budgeting properly prices the programs, develops justification, and an execution plan. Execution performs the approved plan. PPBE has a direct relationship with the Budget-to-Report (B2R) E2E business process. The outputs of P2P, E2E and PPBE are organizational outcomes, and associated financial and non-financial reports. The ERM program assesses the organization's risk while internal controls are implemented to mitigate risk and are inherent throughout execution. IRM is the continuous monitoring of the effectiveness of the risk management and internal controls programs in managing the DON's risk appetite.

In 2018, OMB Circular No. A-123, Appendix A went through a major revision that expanded the focus of internal control reporting assessments from financial reporting to all reports (financial and non-financial) as shown in Figure 2 below.

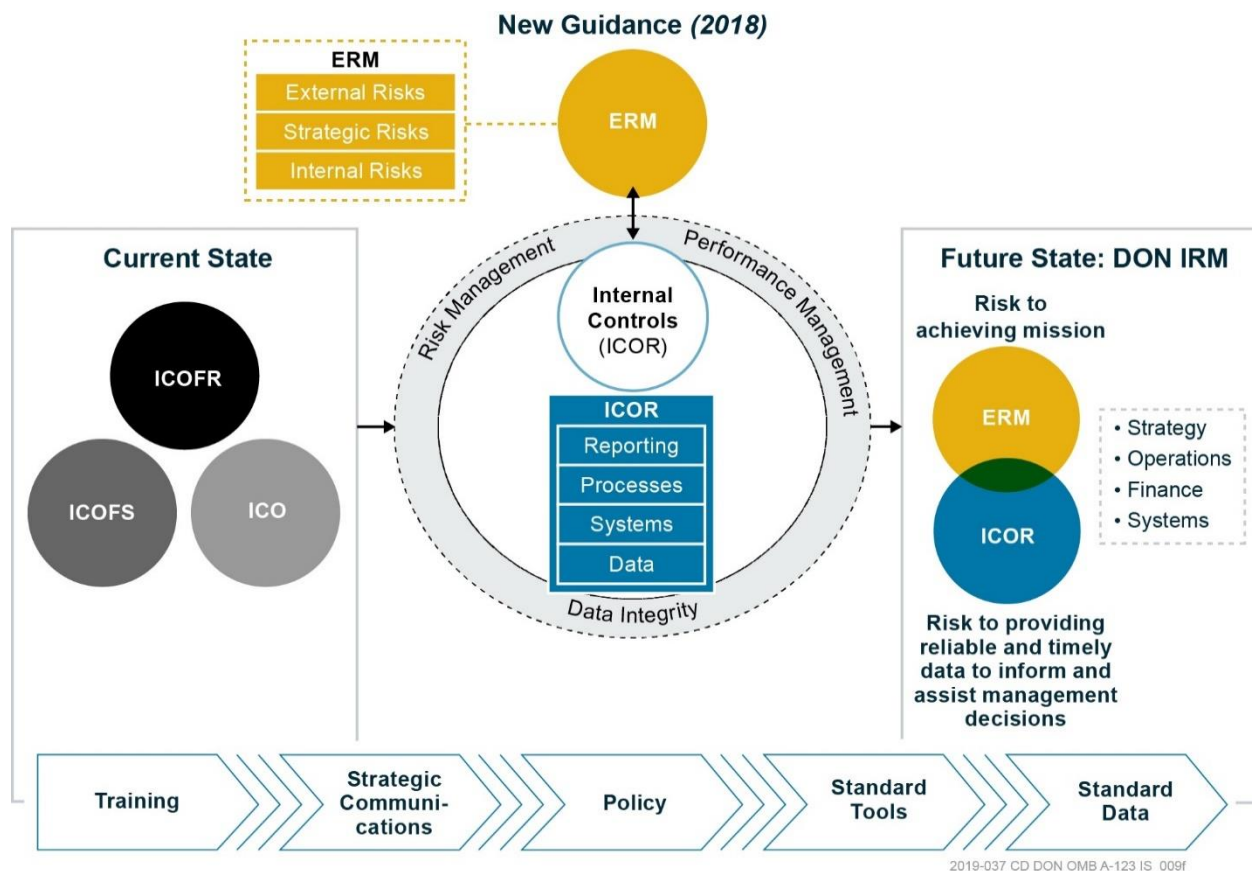


Figure 2. Broadened OMB Circular No. A-123, Appendix A (2018)

This update to Appendix A provides the DON with an opportunity to focus our risk management and internal control efforts on reports beyond just the financial statements to those that impact management decision-making across the DON enterprise.

While this IRM strategy describes the foundation and vision, detailed implementation and execution for the DON will be provided through further guidance as maturity evolves. Historically, the integration points among programs have operated independently (siloe) for consolidation into an overall SOA signed by the SECNAV. The implementation plans for ERM and ICOR will provide concrete steps and timelines for achieving organizational objectives and annual requirements while also transitioning to a more standardized, data-driven, and technology-enabled future state (achieved via integrated enterprise-wide processes). During initial implementation, the DON plans to leverage existing mechanisms for capturing, escalating, monitoring, and managing risks. Over time, the programs will progress along a continuum of maturity, as shown in Figure 3, to provide DON leadership with a holistic and timely view of the risks, performance, and capability to meet the mission and strategic objectives outlined within the DON Business Operations Plan (BOP), as well as other key strategic documents.



Figure 3. DON Integrated Risk Management Maturity Model

Our approach for maturing the DON's risk management capabilities and providing leadership with a proactive means of managing and capitalizing on risk will be driven by four Lines of Effort: People, Processes, Governance, and Technology. Implementing and executing the DON's enterprise-wide business processes, effective internal controls, and a well-designed risk management program will help to mitigate risks of all kinds and achieve the National Defense BOP and DON BOP strategic objectives in alignment with the NDS Lines of Effort. The concept of integrating enterprise-wide business processes tie together the strategic mission, as well as, the operations and finance resulting in an agile, effective, standard, and sustainable holistic approach to risk management and internal controls.

PPBE is the primary resource allocation process for the Department of Defense (DoD) and provides a formal systematic structure for making decisions on policy, strategy, and the development of forces and capabilities to accomplish the BOP. Figure 4 depicts the concept of integrating PPBE, as part of the risk response, to support the achievement of the NDS, business operations objectives, and day-to-day operations to meet the mission.

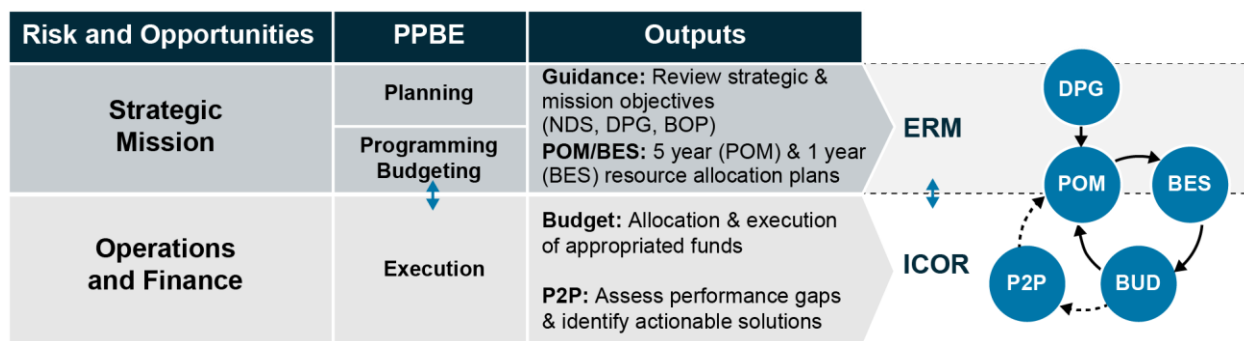


Figure 4. PPBE Process and Impact to IRM Strategy

1. **Planning – Defense Planning Guidance (DPG):** Examines previous guidance to current Presidents National Security Strategy (NSS), SECDEF's NDS, and Chairman of the Joint Chiefs of Staff's (CJCS) National Military Strategy (NMS) to ensure the resulting DPG aligns with the Administration's policy goals. Additionally, the DPG takes into account changing conditions and trends, threats, technology, readiness posture, and economic assessments.
2. **Programming – Program Objective Memorandum/ (POM):** The POM is the funding plan that displays the resource allocation decisions, considering risk of under or over funding programs, for each military service and defense agency covering a 5-year period.
3. **Budgeting – Budget Estimate Submission (BES):** The BES is completed annually and encompasses the first year of the POM, taking into consideration funding and fiscal controls. The budget will be leveraged as a data point to assess execution. The budget of the DON (submitted annually in February) does express in financial terms the plan for accomplishing objectives identified in DON and DoD strategic planning documents. The DON's process supports resource allocation decisions made in turn by BSOs, the SECNAV, the SECDEF, the President, and the Congress. At each phase of the budget cycle, the budget reflects the priorities and the financial plan for achieving the objectives of the decision-maker responsible for that phase. As finally enacted in appropriations, the DON budget serves as a control mechanism to ensure that financial resources are applied to the activities that were approved by the decision-makers in the process. The DON's policy of having BSOs participate in each phase is intended to produce better decisions and to provide those offices with a better understanding of the decisions so that they can better execute the budget.
4. **Budget Execution – Budgeting (BUD):** Allocation and execution of appropriated and revolving funds.

5. **Performance-to-Plan (P2P):** P2P is an enterprise management approach that identifies performance gaps, ascertains barriers to execution, and develops actionable solutions to improve readiness (expanding to other outcomes as program matures). Outcome metrics and corresponding key drivers are identified and defined among subject matter experts and echelon I/II leadership, resulting in a comprehensive, shared understanding of the significant factors driving success. Each outcome metric and driver is designed to be a quantitative measure so that performance can be tracked, modeled, and projected using data analytics, enabling leaders to focus on and prioritize the drivers that have the most impact on improving readiness. Further, this data-driven approach helps inform a more effective allocation of resources and planning.

Background

“Advancing to a Culture of Excellence”

Each Sailor, Marine, civilian, and contractor supporting the DON should be intimately familiar with the DON mission: “**man, train, and equip combat-ready Naval forces capable of winning wars, deterring aggression, and maintaining freedom of the seas**”¹. The DON achieves its mission through the Operating Forces, as well as the Shore Establishment, which is responsible for supporting activities such as communication, training, intelligence, logistics, contracting, acquisition, medical and dental facilities, and maintenance of base facilities, among other responsibilities.

A substantial number of stakeholders across the DON, DoD, and the military-industrial base are involved in achieving these objectives and carrying out these processes. Laws and regulations, in addition to compliance requirements, are also necessary for executing our daily responsibilities to fulfill the mission. Integrating comprehensive enterprise-wide processes, risk management and internal controls is imperative to achieving DON Readiness, which directly drives the change to a culture of excellence with reduced barriers/risks. When variables or constraints are introduced (e.g., the requests to move faster or do more with less) the barriers or risks to achieving the mission objectives grow. Instead of withdrawing from risks, the Federal government and the DON have moved to embrace risk as another “lever” to achieving mission objectives, increasing risk tolerance where appropriate to move more rapidly, and lowering risk tolerance where warranted to achieve more consistent outcomes through risk optimization, as shown in Figure 5.

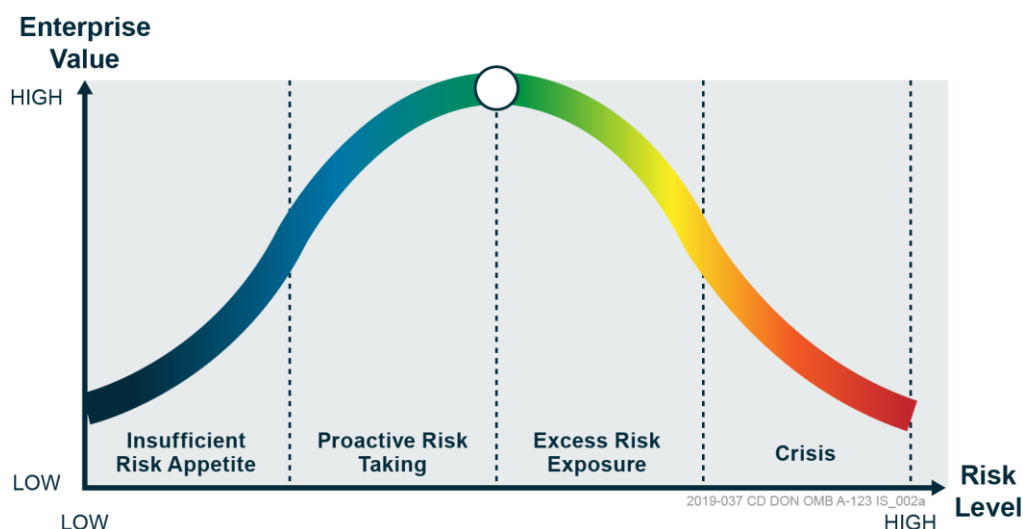


Figure 5. Risk Response Optimization²

The challenge of DON managers was, and is, to balance the **cost** (time, resources, and level of effort) of the risk management mitigation process with the **return** of such efforts, while incorporating consistent processes that are compliant with a plethora of DON, DoD, and federal regulations. The guidance for the DON to employ ERM and Internal Control Programs reside in the OMB Circular No. A-123, “Management’s Responsibility for Enterprise Risk Management and Internal Control.” The section below outlines the requirements for these programs, an approach to help optimize the cost versus return trade-off and the evolving regulations and OMB Circulars, which have provided more flexibility to the Services

¹ Department of the Navy Mission, Vision, and Priorities, August 29, 2017

² Chart: “The Risk-Value Curve: How to Optimize Risk and Generate Value for Your Organization.” Hills, Pankaj, Pashia, and Wallig, *Public Risk*, Jan 2019

over time to continue transforming risk management and internal controls processes to advance a culture of excellence.

Each organization within the DON maintains a vision statement or clearly defined commander's intent – often supported by well-defined priorities and objectives that meet the overall mission of the DON and aligns to the Department-wide and Executive Branch mission (Figure 6 shows several examples). While each of the strategies are promulgated by different leaders, the alignment of the objectives to the NDS is unquestionable. Within the DON, organizations could be considered assessable units where the ERM and ICOR programs would be executed and aligned to the DON IRM.



Figure 6. DON Mission and Vision Examples

Requirements

The requirement for OMB Circular No. A-123 is rooted in several pieces of legislation passed by Congress and signed into law by the President that reinforce the requirements of management to improve the efficiency and effectiveness of government (both financial and mission-related). The most significant legislation impacting OMB Circular No. A-123 are:

- Federal Managers' Financial Integrity Act (FMFIA) of 1982
- Antideficiency Act (ADA) of 1982
- Chief Financial Officers (CFO) Act of 1990
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Government Performance and Results Act (GPRA) Modernization Act of 2010
- Improper Payments Elimination and Recovery Improvement Act (IPERIA) of 2012
- Digital Accountability and Transparency Act (DATA Act) of 2014
- Fraud Reduction and Data Analytics Act (FRDAA) of 2015

OMB Circular No. A-123 was first issued in 1981 and was updated periodically until 2016, when the Circular was rewritten to emphasize the integration of ERM and internal controls in improving mission delivery. The revision in 2016 complemented and expanded the preceding update to OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," which required all agencies to implement ERM as appropriate for the agency mission and in accordance with agency-specific programs. Due to the OMB Circular No. A-123, Appendix A's major revision in 2018 expanding the focus of internal control assessments from financial reporting to all reports, the DON will group these financial and non-financial requirements into ICOR. ICOR will encompass and supersede the categories of internal controls the DON uses today: ICOFR, ICOFS, and ICO. The updated Circular requires the DON and other Executive Branch agencies implement an ERM capability integrated with the DON strategic planning, assessments,

and internal control processes and requires close collaboration with the agency Chief Management Officer and the CFO. Within the DON, these functions are led respectively by the Under Secretary of the Navy (UNSECNAV) and executed by the Office of the DON Chief Management Officer (OCMO), and the Assistant Secretary of the Navy, Financial Management and Comptroller (ASN (FM&C)).

OMB Circular No. A-123 also includes four appendices that emphasize requirements for specific elements of an effective OMB Circular No. A-123 Program:

- Appendix A: Management of Reporting and Data Integrity Risk
- Appendix B: Improving the Management of Government Charge Card Program
- Appendix C: Requirements for Payment Integrity Improvement
- Appendix D: Compliance with FFMA

The Office of the Secretary of Defense (OSD), DoD OCMO and the Under Secretary of Defense (Comptroller) are responsible for implementing and managing the Secretary of Defense's program over internal management controls. The Comptroller's office provides guidance to establish requirements for the preparation of the annual SOA, required by the FMFIA and Department of Defense Instruction (DoDI) 5010.40, "Managers' Internal Control Program Procedures" (MICP). The guidance identifies the DON as a component organization required to submit a SOA to the Secretary of Defense each year.

Specific requirements included in OMB Circular No. A-123 and OMB Circular No. A-11 are:

- Establishing a governance structure to implement, direct, and oversee implementation of the Circular effectively;
- Implementing activities supporting ERM by assessing and managing risk as a part of strategic and data-driven reviews;
- Integrating risk management and internal control functions;
- Developing a maturity model approach to the adoption of an ERM framework and continuously building risk identification capabilities into the framework to identify new or emerging risks and/or changes in existing risks;
- Maintaining a risk profile that provides a thoughtful analysis of the risks arising from DON activities and operations performed to achieve its strategic objectives, and identifying appropriate options for addressing significant risks;
- Assessing the completeness and reliability of the performance data presented and a description of agency plans to improve completeness, reliability, and quality, where needed;
- Leveraging existing offices or functions within the organization that currently monitor risks and the effectiveness of the organization's internal controls; and
- Evaluating the effectiveness of internal controls annually using Government Accountability Office's (GAO's) Standards for Internal Control in the Federal Government (The Green Book).

"All executive agencies are required by OMB Circular No. A-123 to integrate ERM processes and internal controls, and are required to include consideration of internal controls over reporting in their annual assurance statement. This update aligns ICOR with existing OMB Circular No. A-123 ERM efforts. This framework for internal controls over reporting may be phased in over several years as the agency's ERM processes mature. As an agency's ERM processes mature, the agency risk profile may begin to identify and link some enterprise risks with formal internal controls. As this integration occurs, management must include consideration of these controls in the OMB Circular No. A-123 assurance process."

– OMB's Integration and Maturity Guidance
(Appendix A to OMB Circular No. A-123, "Management of Reporting and Data Integrity Risk", – June 6, 2018)

Why Change Now?

DON Leadership continues to emphasize the need for urgent change that will drive the agility and lethality of the warfighter. The current state of our risk assessment and internal control activities are too compliance-oriented and do not necessarily lead to data-driven strategic decisions that improve the management of the DON.

Comprehensive integrated enterprise-wide processes along with effective ERM and ICOR programs are essential to an agile, impactful, standardized, and sustainable DON. They provide for the increased transparency and insight into budget spend, performance and achievement of BOP objectives, and reinvestment, the DON needs to improve readiness and modernization of the Fleet. They streamline reporting requirements and support cross-functional decision-making and trade-off analysis among risks, controls, operations, information technology, and acquisitions, while retaining organizational knowledge within the Navy enterprise for future mission analysis. In other words, in addition to supporting compliance and accountability, risk management is a knowledge management endeavor, ensuring availability of data. The immediate benefits realized when an integrated risk management framework is leveraged across the enterprise include:

“Measuring performance and risk are sound management practices, and must be fully incorporated into the Department’s daily decision-making cycle. We are entrusted by the American taxpayer to be good stewards of their hard-earned dollars – they rightly rely upon us to eliminate inefficiencies and maximize their investment in naval capabilities for their continued security and prosperity.”

– **DON Business Operations Plan FY 2019–2021**

- Transparency of risk and early identification of future readiness concerns;
- Accurate, accessible, and up-to-date data to support planning and executing current and future missions;
- Synergy across the DON by not duplicating problem-solving efforts; and
- Elimination of wasteful hours of administrative burden carried out by valuable resources through better prioritization, standardization, and use of technology.

The June 2018 update to OMB Circular No. A-11 further solidifies the relationship among internal controls, risk management, and agency strategy. OMB A-11 (Sec. 240.27) states:

“By aligning the updated [OMB Circular No. A-123] Appendix A to the agency’s ERM processes, agency management should apply the analysis of risk in the agency’s risk profiles across a portfolio view of the agency’s objectives (e.g., strategic, operations, reporting, and compliance objectives)... when deciding where internal controls will be most effectively employed to those reporting objectives where inaccurate, unreliable, or outstanding reporting would significantly impact the agency’s ability to accomplish its mission and performance goals of objectives... Management decisions to apply ICOR should be made at the individual performance goal and indicator level, applying only in those instances where there is significant risk that a material reporting error may impact achievement of the agency’s mission objectives, and application of ICOR is likely to cost effectively mitigate that risk.”

Based on updated policy, organizational standards, operational mission, and financial regulations, a holistic and integrated risk management and internal control program is necessary. This can only be achieved through uniting risk management, internal controls, and enterprise-wide business processes. The DON’s ERM Program is currently in the informal/foundational (siloeed enterprise-wide processes, internal controls, and risk management) stage and will start progress towards the standardized (collaborative) stage with assessing the risks to achieving the NDS as it relates to accomplishing the major objectives of the DON BOP. Additionally, accountability currently only exists vertically at the business process level, but with an integrated approach, accountability will cover both horizontal and vertical lines of accountability. Although, we already have many effective risk identification, risk assessment, and governance processes at the DoD and DON levels, part of having effective risk management will be assessing whether there are any gaps to inform strategic decision-making.

Current State of Risk Management and Internal Controls

The DON seeks to progress its ERM and Internal Control Programs along a maturity model from its current Foundational (siloed) stage to a fully Optimized (Integrated) stage. The risk and internal control management and assessment approach to-date has been extremely labor intensive and in some cases has produced sub-optimized results due to siloed decision making. The DON has implemented and continues to refine our internal control governance structure to monitor risks, effectiveness of internal controls, and remediation of deficiencies, as well as, to report progress in the annual SOA – with the goal of building the foundation for a strong and effective internal control environment. As the ERM and Internal Controls Programs mature, the governing bodies will reassess the current governance structure for impact, agility, and efficiency. The Business Operations Management Council (BOMC), Audit Committee, and Senior Management Council (SMC) comprise the governing bodies and represent the highest levels of leadership necessary for the establishment of a governance structure to implement, direct, and oversee implementation of the DON Integrated Risk Management Strategy and all the provisions of a robust process of risk management and internal control.

The recent changes to OMB Circular No. A-123 and its appendices – especially Appendix A – as well as OMB Circular No. A-11 have brought about new and expanded requirements that the DON must now develop actionable plans to meet. Our processes and programs with respect to each of the three main areas of focus are at varying levels of maturity:

- **ERM.** The DON OCMO, reporting to the Under Secretary, is in the very early stages of establishing an ERM Program and a framework for managing enterprise risks. Once established, OCMO will administer the DON ERM Program and sustain our ERM operations. OCMO is in the process of developing an ERM Concept of Operations (CONOPS) that will establish the guiding principles, roles and responsibilities, and primary processes that will enable the creation of a DON risk profile, management of risk portfolios across the enterprise, and the aggregation of risk insights to assist leaders in achieving the DON's strategic objectives in the BOP, as well as identify internal and external enterprise-level operational and strategic risks, including major reputational risks.
- **ICOR.**

Financial: The DON Office of Financial Operations (FMO), under the ASN (FM&C), administers the DON Managers' Internal Control Program (MICP) and provides guidance, implementation plans, training and assessment support and reviews to the relevant Major Assessable Units (MAUs), Assessable Units (AUs), and sub-Assessable Units (sub-AUs) pertaining to ICOFR, ICOFS, and ICO. The DON MICP has taken on additional activities that span the requirements of OMB Circular No. A-123 Appendices A, B, C, and D, in addition to assessing Entity Level Controls (ELCs), the review of MAU, AU, and sub-AU certification statements, and preparation of the SOA. Those assessments, however, lack consistency as the MAUs, AUs, and sub-AUs vary in their level of maturity in documenting and performing risk and internal control assessments. As cited by the DON's Independent Public Accountant in November 2018, the DON MICP in its present form and function has not achieved compliance with OMB Circular No. A-123. The finding asserts that several key Circular A-123 program requirements, to include a Risk Profile, Process Cycle Narratives, and detailed internal control testing guidance for Budget Submitting Offices (BSO) were not in place and fully operational in FY18.

Operational: The MAUs, AUs, and sub-AUs conduct a series of operational reviews that start with consideration for the DON's mission, the BOP and the respective mission and objectives of each MAU, AU, and sub-AU. The MAUs, AUs, and sub-AUs identify risks to achieving their missions and objectives, develop risk response strategies that may call for new or stronger internal controls, conduct operational program assessments, and report on their results. Those results feed the DON's current reporting on ICO in the Secretary's annual SOA. However, these operational reviews do not follow a standard, consistent approach supported by uniform tools, templates, and terminology. They are more reflective of a bottom-up risk management review consistent with the Departments distributed command and control structure but are not designed to meet the recently expanded requirements of OMB Circular No. A-123, Appendix A to all facets of reporting, data quality, and

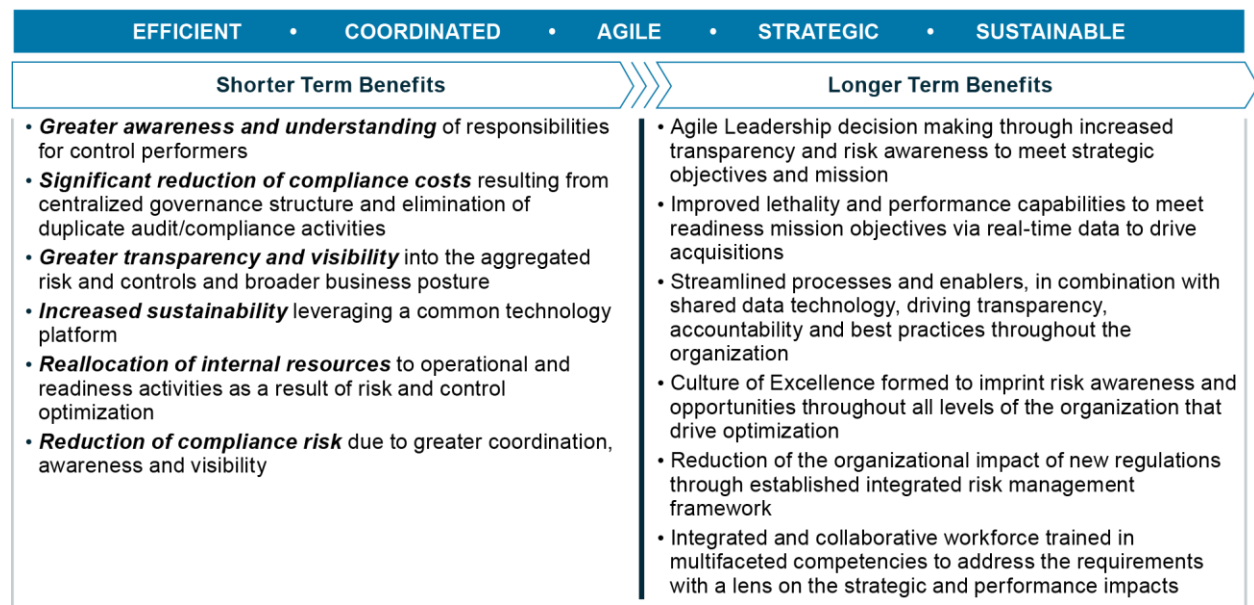
assessment of business system controls (beyond just financial reporting) that support management decision-making.

The DON's annual assessment activities culminate with the DON MICP drafting the annual DON SOA for the SECNAV based on individual Certification Statements prepared by MAUs, AUs, and sub-AUs. The DON MICP conducts limited analyses to identify overall DON-wide trends and gaps across the submissions to help prepare the specific SOA content and, ultimately, determine the level of assurance regarding the effectiveness of the DON's system of internal controls. DON-wide Material Weaknesses (MWs) and Significant Deficiencies (SD) identified in the SOA require corrective action plans (CAPs) to be recorded in the DON's Deficiency Tracking Tool (DTT), where CAP progress can be tracked and reported in the SOA. In its present state, the DON's SOA is largely a consolidation and aggregation of individual Certification Statements drafted, signed, and submitted by the MAUs and BSOs (bottom-up approach). It is not prepared based on the collective internal control assessments and risk management activities conducted across the DON. Not until the DON's respective ERM and ICOR programs reach a greater stage of maturity and integration as well as cover the full set of requirements in OMB Circular No. A-123 and its appendices, can the SOA provide a complete and accurate reflection of the DON's system of internal controls.

Benefits of Integrated Risk Management

Leaders in any organization require timely insight into their environment to enable the most effective decision-making to achieve their mission objectives. Integrated enterprise-wide processes are the essential link to an agile, effective, standard, and sustainable ERM and ICOR program. Robust ERM programs serve as a catalyst for organizations to identify, assess, aggregate, respond to, and monitor risk conditions effectively, to allow leaders to anticipate events that could have an impact on the achievement of the most significant enterprise goals. As OMB Circular No. A-123 emphasizes the need for integration of an organization's ERM framework and its risk-based approach to internal control programs and activities, the benefits created will have an exponential impact throughout the organization. An integrated approach to ERM incorporates financial, strategic, and operational pillars to holistically identify and mitigate risk to meet the DON BOP.

Benefits will be realized by the DON in phases (shown in Figure 7), similar to the maturity model presented earlier within this section and in Appendix A of this document.



2019-037 CD DON OMB A-123 IS_006e

Figure 7. Benefits of Integrated Risk Management

Although, the short-term benefits will create an immediate impact to allow integrated communications and reporting structures, the long-term benefits align to the future-state vision that realizes the advancement to a culture of excellence.

Vision for the Future State

In order to shift from Current State to Future State, training, communications, new/modified policies, tools, and data management will be developed by the DON to support this journey. Consistent with leading standards and frameworks, the DON's Internal Control Program will be incorporated as a part of the Department's broader risk management process, while complementing the expanded OMB Circular No. A-123, which is focused on integrating risk management with strategy setting. It stands to reason that, if internal controls and risk management are to be integrated and ERM is integrated with strategy and performance, then the DON's Internal Control Program, having been elevated, should have a direct and impactful connection to the Department's strategy setting and operational performance. At the center of ERM and ICOR are comprehensive enterprise-wide processes supporting a holistic approach to assessing risk across the organization and business processes, efficiency, risk identification and mitigation, standard and accurate metrics, and an effective data management strategy. To reach maturity in an ideal state for integrated risk management, the DON will have the programs, processes, structures, and technologies in place to manage risks, reduce burdensome compliance activities, and drive a culture of agility, high performance, and capabilities excellence.

Effective ERM and ICOR permeates all layers of the organization and processes, providing the mechanisms to share risk insight to all relevant stakeholders throughout a decision-making value chain. It relies on both top-down and bottom-up components, typically enabled by a centralized function that establishes the foundational capabilities and provides the conduit to capture and share risk insight at the enterprise level of the organization. The top-down elements require active engagement by senior leaders to create the environment where risk information will be embraced when shared, and use of the information upon which to base strategic enterprise-level decisions. The bottom-up portion of ERM represents the eyes and ears of risk identification, as well as the primary responsibility for the management and response to identified risks. The value proposition of ERM cannot be fulfilled without active engagement from all parts of the organization.

Importantly, the relationship and flow of influence among internal controls, risk management, and the DON's strategy and operational performance is bidirectional with enterprise-wide processes as the integration center. In a fully mature, integrated environment, ERM enhances strategy selection – refinements to the DON strategy call for structured decision-making that analyzes risk and aligns resources with the mission and NDS. Significant and/or widespread internal control failures identified through the DON's Internal Controls assessments can contribute to, or become, enterprise risks to the DON, which in turn could influence the DON's strategy and objectives within the BOP as they are reviewed and updated.

In the other direction, a lack of measured progress toward attaining BOP objectives may point to one or more enterprise risks that are impeding achievement of the strategy. In some cases, the DON can then look to its Internal Control Program to evaluate the controls in processes and systems associated with the programs that contribute to that objective and, where needed, invest in strengthening/improving those controls to mitigate that risk. In short, the ERM Risk Profile should influence the scope of the DON's internal control assessment and remediation activities.

Collectively, the DON's risk profile and internal control assessment results will shape resource management, investment, and acquisition decisions from the DON's most senior decision-making bodies. Assistant Secretaries and Senior Departmental leadership would present the highest-priority risks or issues that need to be resourced to a decision-making body – like the BOMC – to consider among the Departments full set of investment needs. These efforts can become business objectives incorporated into the BOP that get measured and reported on as part of the DON's annual priorities.

How We Get There – Maturity

The DON's ERM and ICOR programs are still maturing; similar to other big and multifaceted organizations establishing complex programs, implementing ERM and Internal Controls, including the change to reporting (ICOR), programs are a continuous effort – building on existing efforts. Substantial work remains to establish, define, and improve their respective functions. Initial integration can be achieved through establishing linkages early on and maturing through continuous collaboration. As the DON's ERM and ICOR programs mature, a concerted effort to identify and build the connection points that tie together the DON's internal control and risk management activities will take place. For instance, it will be imperative to tie PPBE, P2P, and E2E business processes together with ERM and ICOR to achieve an agile, effective, standard, and sustainable integrated risk management program. A mature and integrated ERM and ICOR program will result in more accurate metrics providing a true assessment of readiness while keeping all stakeholders accountable.

The DON seeks to progress along this continuum of maturity to achieve the Integrated State summarized in Table 1 (the expansive model encompassing the programs and integration is located in Appendix A). Each stage can be characterized by marked advancements first in individual ERM and ICOR program functions, and eventually in the four lines of effort – People, Processes, Governance, and Technology – that tie them together to achieve full operational maturity and integration in an optimized state. Mature programs will generate accurate Readiness metrics required to meet the DON strategic, organizational, and financial missions.

Lines of Effort

Proper implementation of the four Lines of Effort will empower the DON to roll out a successful Integrated Risk Management framework, manage risks to enable the achievement of its objectives, and improve agility and Fleet readiness through improved transparency and data-driven decision-making capabilities.

- **Line of Effort 1 – People.** Managing the cultural change across the organization does not mean simply promulgating training periodically on concepts around risk management. Instead, securing the buy-in of a reasonably skeptical organization will require the DON to take a multifaceted approach that includes setting the tone at the top across all Echelons, incorporating risk management into Navy and Marine Corps schoolhouse curricula, identifying early adopters to demonstrate success stories, and developing a replicable model across the DON.
- **Line of Effort 2 – Processes.** The DON's integrated risk management structure will balance risk response and compliance requirements to alleviate burdensome and paper drill activities. Our approach includes establishing standardized, data-driven, and technology-enabled processes to support and enhance our strategy by facilitating transparency of risk insight to the right level of the organization as early as possible.
- **Line of Effort 3 – Governance.** Our approach will implement and sustain a governance structure within the DON that provides opportunities to identify, monitor, and manage risks and, where needed, take corrective actions both up and down the chain of command and across similar enterprise functions, inclusive of operational, financial, and enterprise risks.
- **Line of Effort 4 – Technology.** While the DON recognizes that technology is an enabler of a sound risk management program, we also understand the frustration of the organization if manual processes are developed that remove our men and women in uniform from achieving their core mission. That is why we have included identification and piloting of technology solutions as a separate line of effort to support and enhance program maturity. Our technology solutions enable continuous risk identification and response capability and will help to accelerate the DON's adoption and the effectiveness of the overarching program by eliminating manual processes that take away and cause frustration amongst leadership and program owners.

Table 1. Goal End-state of the DON Integrated Risk Management Maturity Model*Key: People (P), Processes (Pr), Governance (G), and Technology (T)*

Program Areas	Requirements Met	Sustained/Optimized (Integrated)
Enterprise Risk Management (ERM)	OMB Circular No. A-123 (Overall) OMB Circular No. A-11, Sec. 260.23, 260.27, 260.28	<ul style="list-style-type: none"> • Leaders and other employees take a risk-based approach to making decisions, thereby, increasing, adopting, and promoting risk transparency (P) • Standard ERM capabilities and practices are adopted and continue to evolve and improve, with adoption across the enterprise and integration into the DON's mission operations (Pr) • All governance throughout the organization embraces risk insight for decision making, investments, and strategy (G) • Executive champions drive importance of aligning ERM to service delivery and DON strategic objectives (G) • Integrated technology platform deployed to capture and integrate other risk program data from within and outside the enterprise (T)
ICOR	OMB Circular No. A-123 (Overall) and Appendices A thru D OMB Circular No. A-11, Sec. 240.26	<ul style="list-style-type: none"> • Professionals with defined, well-understood roles throughout internal control lifecycles receive consistent and effective training from Internal Control Program leaders/coordinators (P) • Integrated and effective processes and system controls are in place enterprise-wide to provide assurance over all facets of the DON's most significant financial and non-financial reporting; management monitors progress and effectiveness in real-time (Pr) • Routine monitoring is performed as part of a structured, risk-based program over key processes and system controls that support management reporting (Pr) • All senior leaders, governance and operational community embrace risk management and operational internal control accountability to influence and direct DON operations (G) • Customized decision support tools are integrated with each other and with external data sources that support forward-looking risk indicators and tie to control performance (T)
Integration Points	OMB Circular No. A-123 (Overall) OMB Circular No. A-11, Sec. 240.27, 260.27	<ul style="list-style-type: none"> • "Tone at the Top" is mirrored and embraced at all levels of the Department; internal controls and risk management are part of daily operations and understood as valuable to the mission (P) • Preparation of the SOA is a coordinated effort between Internal Control and ERM Program leaders (i.e., SOA is based not only on individual MAU/BSO certifications, but the collective ERM and internal control assessment results reported by OCMO and FM&C) (Pr) • Senior-most governing and decision-making bodies use risk and internal control information, alongside other operational performance data, to make risk-based management decisions on investment of Department resources to risk and remediation activities (G) • Enterprise Governance Risk and Compliance (eGRC) tools integrate disparate risk/compliance management initiatives and help automate risk and internal control activities across the Department (T)

People

Integration cannot be achieved by processes alone; the people who drive those processes and are impacted by them are the most critical element in driving a successful integration strategy. These changes represent an operating and cultural shift that can take time to achieve. As the DON's ERM and ICOR Programs mature, the organizations with primary responsibility for executing those programs must communicate frequently with each other and become increasingly coordinated in their communications to the MAUs, AUs, and sub-AUs. Where individual communications are needed (e.g., from FM&C or OCMO directly), DON organizations must be careful to ensure consistency and alignment in messaging.

Managing the pace of change is equally important for the DON organizations overseeing and executing the programs, as it is for the MAUs, AUs, and sub-AUs who will be on the receiving end of every new

requirement, program change, new or revised assessment tool or template, and reporting expectation. Any increase in requirements or responsibility needs to be resourced. Our organizations do not have the excess capacity to ramp up these functions immediately; we will undertake them progressively and responsibly.

Key Stakeholders and Functional Responsibilities

The SECNAV leads the DON and is subject to the authority, direction, and control of the Secretary of Defense. The Office of the SECNAV shall have sole responsibility across the Office of the SECNAV, Office of the Chief of Naval Operations (OPNAV) and Headquarters, Marine Corps for various functions to include strategic direction, performance oversight, and enterprise-wide risk and response decisions. The SECNAV is the final approver of the SOA, assuring compliance of OMB Circular No. A-123 requirements are met by the DON.

The UNSECNAV shall perform such duties and exercise such powers as the SECNAV may prescribe. This includes the establishment of the framework to implement the DON strategy for ERM and Internal Controls. The UNSECNAV approves and assigns members to leadership committees, councils, and boards as needed. The responsibilities of the UNSECNAV include:

- Sponsor/owner of the Integrated Risk Management strategy within the DON
- Chairs BOMC and Audit Committee and sets overall direction of DON Integrated Risk Management

OCMO and OASN FM&C provide oversight and accountability of the DON ERM and Internal Controls initiatives and are considered the enterprise-wide system champions to reduce risk through reporting requirement consolidation. Their role is best understood as that of integrator and administrator and serve as a single point consolidator and evaluator of Risk Management and Audit Compliance for the DON.

OCMO has a unique charge in establishing, deploying, and maintaining the DON's ERM Program and sustaining ERM operations. Specifically, OCMO will be establishing and maturing the DON ERM Program. They are responsible for drafting, maintaining, and finalizing the DON Risk Profile containing enterprise risks and response strategies. Leading in this regard requires providing coaching and support on implementing and performing ERM activities (e.g., tools/templates, training).

OASN FM&C will maintain a core focus primarily on internal control assessment activities across OMB Circular No. A-123, Appendices A thru D, Fraud Risk and ELCs. FM&C will be responsible for maturing the financial portion of the DON ICOR Program, which means they are also responsible for assessing the financially relevant systems, directly compiling and consolidating the data within the DON financial statements and additional material financial reports. The responsibilities of the FM&C include areas of overlap where integration and collaboration must occur:

- **ICOR.** Changing requirements (OMB Circular No. A-123 and revised Appendix A) have pushed reporting beyond ICOFR and called for operational risk and assurances to take on greater importance than before in the SOA. This will require the DON to assess reports beyond the financial statements that are considered material with the associated business system internal controls.
- **Fraud Risk Assessment.** There are financial and operational components to this; the BSOs and the MAUs will both move out on a portion of the assessment and provide results up to FM&C, then FM&C will synthesize those results to produce an overall fraud risk profile for the DON that spans both operational and financial considerations.
- **ELCs.** The completion of ELC assessments across the DON extends to all MAUs and, by nature of the assessments, requires input from the senior-most officials in those units. MAUs are likely in the best position to lead evaluation of all 17 Green Book principles at this point in time. As FM&C's capabilities expand and the ICOR Programs advance, FM&C can begin to use internal control assessment results it collected and synthesized from across the Department to evaluate

effectiveness of the DON's "Control Activities" activities without the MAUs needing to focus on that aspect of the ELC assessment.

- **Statement of Assurance.** Preparation of the SOA requires direct input in the form of the assurances to include DON's internal controls, risk profile, enterprise-wide assessments, and remediation efforts, resulting in capturing inputs from a broader community outside the financial boundaries.

FM&C will lead E2E financial process assessments for ICOR and Information Technology General Controls (ITGC) and Application control assessments. FM&C will also lead IPERIA and Government Charge Card assessments (Appendices B & C). Leading in this regard requires providing a full suite of support to the AUs that will be responsible for executing on the assessment requirements (e.g., tools/templates, training, commitments to completion dates).

MAUs/AUs/sub-AUs support the implementation and integration of the DON ERM and Internal Controls Programs within their respective organizations. Additionally, they develop, implement, monitor, validate, and report on CAPs to ensure remediation of MWs and SDs. The MAUs, AUs, and sub-AUs gather and manage risk at a tolerable level, report to the Senior Assessment Team (SAT), and assist in enforcing accountability at all levels. The responsibilities of the MAUs, AUs, and sub-AUs include:

- Implementation and execution of programs across the DON
- Provide guidance and training to lower units
- Representatives on and report to the governance bodies

Naval Audit Service (NAVAUDSVC) will serve as an internal auditor in support of the DON ERM and Internal Control Programs. Deficiencies and recommended actions identified by the NAVAUDSVC as a result of audits performed may assist in the identification and mitigation of risks throughout the DON. Generally within the scope of the NAVAUDSVC performing an audit or engagement and reporting results, the NAVAUDSVC may:

- Assess programs, operational units, or areas identified by management that could pose a risk to achieving the DON mission
- Validate controls for sustainment purposes
- Evaluate corrective actions, report findings, and conclusions to the audited entities' governance bodies

As the DON Audit Liaison, NAVAUDSVC provides oversight, coordination and follow-up of external audit activities to ensure timely, quality updates and final closure of audit recommendations.

Naval Inspector General (NAVINGEN) will serve as independent verification and quality control in support of the DON ERM and Internal Controls Programs. These independent assessors will investigate potential risks throughout the DON.

Processes

Integrating the assessments of the enterprise-wide business processes lays the foundation for utilizing standard and efficient reviews resulting in more accurate and comprehensive results, information and understanding of the current internal control environment posture. Standardization has been an ongoing effort within the DON starting with the E2E business processes, along with P2P, due to the pervasive impact to strategic, operational, and financial objectives of the DON. The DON will focus on progressive improvements to its assessment, reporting, and decision-making processes that bring us closer to achieving the following:

- **Standardized Assessment Activities and Integrated Teams.** For each of the core areas in the future state (ERM and Internal Controls), the DON will develop and deploy standardized approaches, terminology, tools, templates, and structures for performing assessments consistently across the

enterprise. Risk management activities (identify risks, analyze and evaluate, develop risk responses, respond to risks, and monitor and review) and the DON's risk profile will help scope the DON's program and control assessment activities. DON organizations that are responsible for different pieces of the same assessment (e.g., fraud risk assessment, operational and financial pieces) will coordinate their planning and assessment activities and synthesize results into a single, cohesive output. The overall assessment teams will be comprised of personnel that, together, understand the financial and operational aspects of the DON's enterprise-wide business operations and the assessment objectives. Integrated assessment teams and activities will help to avoid duplication of assessment efforts and minimize disruption to the MAUs, AUs, and sub-AUs.

- **Integrated Assessment and Reporting of Results.** The standardized approaches, tools, and templates deployed for assessments will pave the way for more effective and insightful analyses of assessment results across the Department to identify where DON management's attention needs to be most focused. Reporting to Department leadership, Congress, oversight bodies, and the public will be more consistent and integrated. Preparation of the SOA will be more methodical and defensible; it will be based not only on individual certifications provided by MAUs, AUs, and sub-AUs, but the collective risk profile and internal control assessment results observed and reported on by OCMO and FM&C, respectively, throughout the year.
- **Integrated Governance and Decision-Making.** At the senior-most levels in the organization, the BOMC will use risk and internal control information – alongside other operational performance data – to make risk-based and informed management decisions to prioritize, align, and invest DON resources in addressing those that are most important. The BOMC will be informed by the Audit Committee and SMC to employ a data-driven decision-making process based on an embedded risk-based approach.

Governance

Governing bodies must be reassessed for appropriate stakeholder presence and will depend upon the realignment of MAUs, AUs, and sub-AUs. The overall governing bodies may be consolidated, expanded, and/or member realignment will take place to ensure that the DON IRM Strategy has necessary level of leadership, sponsorship and decision maker support required to address strategic and mission related risks. Once the governing bodies are established, they will be imperative to the success and integration of the DON IRM Strategy.

Technology

The BOP (Strategic Objective 3.1.A) emphasis on increasing the use of data analytics and other advanced technology platforms (e.g., artificial intelligence, robotic process automation) in DON-wide decision-making extends to the Department's risk management and financial operations enterprises.

"Always scanning the horizon for new technologies and ways to do our business better will lead to greater agility to meet emerging threats."

– **DON Business Operations Plan FY 2019–2021**

The DON prioritizes the use of technologies that improve visibility and accountability and promote better data and risk-based decision-making in an environment where business controls enable faster, more informed decisions³. The BOP also calls for investments and improvements in the DON's overall enterprise data quality, standards, and integration. As data availability and quality improve, the integration between operational and financial data will also improve influence other systems and the impacts of the DON's reporting and management decision-making. As clear technology requirements are established for the DON IRM Strategy, a tool will be selected with an eye towards leveraging technology to optimize integration, efficiency, automation, and ease-of-use to accelerate maturity.

³ 2018 DON Business Operations Plan, p. 33

Dashboard and Performance Reporting. Dashboards and reports will be tailored for presentation to and use by governing bodies and DON Leadership. Existing tools may be leveraged or expanded upon and others may be newly developed. The DON will build out modules that digitize each of the OMB Circular No. A-123 Appendix A thru D assessment functions – providing electronic forms and workflows for assessment teams to conduct their evaluations in a standardized, consistent manner; supervisors and management team members to review and approve testing results; and reporting of assessment results in standard templates. That level of consistency and standardization will drive the DON's ability to quickly view assessment results and Department performance across E2E business processes to pinpoint enterprise-wide risks that need more immediate escalation and response.

Advanced Data Analytics. Over time, the DON will employ and configure analytics platforms to significantly increase our capability and capacity for ingesting and analyzing large sets of transactional data, uncovering errors and anomalies that need to be investigated and corrected, as well as identifying potentially alarming systemic issues that require greater management attention. This will strengthen the DON's audit readiness posture through a program focused on continuous audit readiness. Greater analytics capabilities will also improve individual MAUs, AUs, and sub-AUs ability to report on performance indicators and identify troubling trends related to achieving their specific objectives in the BOP.

Enterprise Governance, Risk, and Compliance (eGRC) Technologies. In the initial stages of integration, the DON will leverage existing technologies and identify opportunities to further integrate and automate activities to produce efficiencies. As the programs mature, the DON will consider investments in a more robust and capable eGRC tool. True eGRC tools integrate disparate risk and compliance management initiatives, providing a single "source of truth" and help to automate risk and compliance management processes across the Department.

Next Steps

The transformation's success is contingent on a well-resourced, well-planned course of action, which will include several major near-term milestones.

Reassessment of MAUs and AUs (People). The DON has a total of 17 MAUs in the current state, defined in most cases by major operating units. In some cases, the MAUs are also business process owners. A reassessment of the DON MAUs, AUs, and sub-AUs will be necessary to ensure the stakeholder communities are properly captured. The MAUs will be defined by operational oversight and E2E business process ownership. Each MAU, AU, and sub-AU will need to establish its own risk and internal control program governance structure to align with the DON-level programs. The DON IRM framework will be taking steps to assist in the management of the performance objectives of the MAUs, AUs, and sub-AUs.

MAU, AU, and Sub-AU Integration and Implementation Support (People). The implementation will require significant training for the MAUs, AUs, and sub-AUs. On-site support and training for stakeholders, in addition to a library of tools and templates, will lend itself to a standardized risk approach, standardized control testing and corrective action development. Possible tools can include playbooks, standard templates for documenting and assessing risks, process cycle memoranda, risk control matrices, internal controls, test plan procedures, and sampling and testing guidance. Continuous monitoring and progress reporting will be based on periodic assessment of the Integrated Risk Management program activities (ERM and Internal Controls) against the maturity model described previously, with each assessment producing discreet actions necessary to move the organization to the next level of maturity. Training and implementation support will be delivered with a focus on the overall execution of DON mission, allowing the integration of risk information to occur vertically and horizontally throughout the DON.

CONOPS and Implementation Plans (Process). There are multiple elements to the proposed transformation, including ERM and Internal Controls and ICOR transition. A CONOPS for each program must be developed in the context of DON operations and regulatory deadlines, namely the deadlines for the annual SOA. Each CONOPS will require defining the scope of the program, relevant knowledge references as appropriate, operational descriptions of the program, and supporting elements detailing the operational and support environments for each program, to include various operational scenarios. Each CONOPS seeks to answer the "Five W's":

- **Who** are the stakeholders involved and their roles?
- **Why** are we establishing these programs at this time?
- **What** are the known elements and the high-level capabilities of the ERM and ICOR?
- **When** will the activities be performed and in what sequence?
- **Where** are the geographical and physical locations of the programs?

Implementation Plans will provide the "How" for each CONOPS through detailed guidance and additional references, tools, and templates. The CONOPS and Implementation Plans will be reviewed and assessed annually to address maturity, organization, and requirement changes that may have occurred and followed by training customized for the various stakeholders throughout the organization.

Reestablish Governance Bodies and Cadence (Governance). Governance will play a crucial role in the new risk management framework, and as such its membership should be reconsidered and reengaged. This may mean identifying new points of contact; it may mean securing the continued commitment of points of contact already on the governance bodies. The DON Internal Control Program will provide coordination and oversight for the SMC and MICP Coordinator Support.

Defining Tools and Enablers (Technology). The DON will leverage a variety of technologies at each stage of maturity. In our current state, the DON's operations, people, data, and systems are not ready to take advantage of sophisticated enterprise tools. However, there are technologies that can be implemented today and, in turn, can assist in maturing the DON's readiness incrementally through advanced tools. In addition to commercially available tools and leading practices from other federal agencies, there are a number of tools and leading practices within the DON that can be leveraged and should be considered. Once the analyses of alternatives have been completed, stakeholders will be engaged to select the tool or set of tools and establish a roll-out timeline to be leveraged in the early stages of integration.



Appendix A. Maturity Model

Table 2. DON Integrated Risk Management Maturity Model
Key: People (P), Processes (Pr), Governance (G), Technology (T)

Program Area	Informal/Foundational (Siloed)	Standardized (Collaborative)	Managed/Monitored (Informed)	Sustained/Optimized (Integrated)
Enterprise Risk Management (ERM) OMB Circular No. A-123 (Overall) OMB Circular No. A-11, Sec. 260.23, 260.27, 260.28	<ul style="list-style-type: none"> Generic to basic knowledge of ERM; no mandate from DON leadership to establish a risk-aware mindset (P) Risk assessment and response are <i>ad hoc</i> and inconsistent across the DON; risks are not viewed across the enterprise (Pr) Resources spent reacting and responding; too busy “fighting fires” to prevent them (Pr) No formal governance of the ERM Program; some risk governance exists, but only within individual entities (G) Manual to non-existent technology, capturing risk data in spreadsheets within individual DON units or programs (T) 	<ul style="list-style-type: none"> A Chief Risk Officer or equivalent role is established and filled to lead program development and execution and advise DON leaders (P) Risk management training provided to DON personnel with formal ERM Program roles (P) Personnel actively using risk management techniques in individual programs/units to conduct business activities (P) Standard ERM processes are defined within individual sub-organizations or units (Pr) ERM responsibilities are formally codified within individual roles, and liaisons to DON management and governing bodies established within major business units (Pr) Risk governance structures are standardized within units and begin collaborating on risk management activities (G) Enterprise-wide risk-focused technology platform (e.g., SharePoint tool, database) selected and beginning to capture risk information (T) 	<ul style="list-style-type: none"> Risk management training provided to broader DON workforce (P) Awareness across the DON of ERM and its value to the Department and mission; managers share information about risks and risk responses continuously (P) Standard ERM capabilities and practices are defined and adopted for the DON (Pr) Risk profile and risk assessment results are shared with OMB as a component of the Summary of Findings (Pr) Governance operating at multiple tiers in the organization with ERM central governance at each layer of the enterprise. Timely risk insight is actively used in decision-making in pursuit of achieving objectives (G) ERM risk profile and assessments interact with DON performance and strategy across technology platforms (T) Use of analytics platforms and reporting to view backward-looking performance measures and some limited forward-looking risk indicators (T) 	<ul style="list-style-type: none"> Risk managers and other employees take a risk-based approach to making decisions, thereby, increasing, adopting, and promoting risk transparency (P) Standard ERM capabilities and practices are adopted and continue to evolve and improve, with adoption across the enterprise and integration into the DON's mission operations (Pr) All governance throughout the organization embraces risk insight for decision making, investments, and strategy (G) Executive champions drive importance of aligning ERM to service delivery and DON strategic objectives (G) Integrated technology platform deployed to capture and integrate other risk program data from within and outside the enterprise (T)



Table 2. DON Integrated Risk Management Maturity Model
 Key: People (P), Processes (Pr), Governance (G), Technology (T)

Program Area	Informal/Foundational (Siloed)	Standardized (Collaborative)	Managed/Monitored (Informed)	Sustained/Optimized (Integrated)
Applicable Requirements				
ICOR				
OMB Circular No. (Overall) and A-123, Appendices A thru D	<ul style="list-style-type: none"> Insufficient workforce capability and/or capacity to achieve control objectives; minimal training for workforce on performance and assessment of controls (P) Responsibilities for internal control are not clear and formalized within individuals' roles (P) No clear approach for applying ICOR to non-financial reporting or selecting the most significant management reports for evaluation (Pr) System and process controls for major reporting mechanisms not fully identified or assessed to determine if they are designed and in place (Pr) Control activities are designed and in place, but inconsistent in documentation and implementation (Pr) Control assessments are inconsistent across the Department and some processes may not be tested; therefore, some control gaps are unknown (Pr) Relatively simple tools operating for discreet functions (e.g., tracking assessment results and remediation progress) (T) Duplicative tools and technologies used for the same purpose in different parts of the organization (T) 	<ul style="list-style-type: none"> Internal Controls responsibilities formally codified in individual roles within A-123 Program functions and across the enterprise (P) Individual roles within A-123 Program functions and across the enterprise (P) Rationale and approach for ICOR is clear and documented (Pr) Management reports where material reporting errors or deficiencies would impact achievement of the DON's mission objectives are identified and selected for applying ICOR (Pr) Data Quality Plan for achieving objectives of the DATA Act (i.e., controls for spending reporting) has been developed and processes are in place for reviewing annually (Pr) Baseline ICOR assessments (including identification of all data, system, and process inputs) performed for the most significant/material DON management reports (Pr) Structures, approaches, tools/templates, and plans are in place for conducting ICOR assessments within MAUs (and BSOs if applicable) (Pr) ICOR activities largely designed and in place, but not consistently documented and implemented; periodic testing is not performed (Pr) Control activities largely designed and in place, but not consistently documented and implemented; periodic testing is not performed frequently enough to identify and resolve errors in timely manner (Pr) MAUs and E2E processes are validated and provide full coverage of Department financial and non-financial processes (Pr) 	<ul style="list-style-type: none"> Knowledgeable workforce with capacity in place to properly execute controls and perform assessments consistently (P) Control activities for financial and non-financial reporting are consistently documented and implemented, periodic testing is performed (Pr) Assessment planning and scoping consider changes to DON business operations and reporting activities to identify new reports for ICOR baseline assessments (Pr) ICOR assessments performed for full range of the DON's most significant/material management reports using standardized tools/templates across the Department (Pr) Assessment results are analyzed and evaluated at the Department level to identify enterprise-wide reporting weaknesses for reporting to SMC and other governance bodies (e.g., BOMC) (Pr) Assessments covering ICOR objectives – including charge cards (Appendix B), improper payments and recovery (Appendix C), fraud risk, and ELC assessments are consistently performed using standardized tools/templates across the Department (Pr) Responsibility for ICOR requirements rests with senior leaders or governing body (e.g., CNO/CMC) with sufficient authority and influence to direct DON operations (G) Internal financial/non-financial/operational data is accessible and reliable to feed 	<ul style="list-style-type: none"> Professionals with defined, well-understood roles throughout internal control lifecycles receive consistent and effective training from Internal Control Program leaders/coordinators (P) Effective process and system controls are in place enterprise-wide to provide assurance over all facets of the DON's most significant financial and non-financial reporting (Pr) Routine monitoring is performed as part of a structured, risk-based program over key process and system controls that support management reporting (Pr) All senior leaders, governance and operational community embrace risk management and operational internal control accountability to influence and direct DON operations (G) Integrated Risk Management Program provides oversight and facilitation support for the SAT and coordination and oversight for the SMC (G) Customized decision support tools are integrated with each other and with external data sources that support forward-looking risk indicators and tie to control performance (T)



Table 2. DON Integrated Risk Management Maturity Model
 Key: People (P), Processes (Pr), Governance (G), Technology (T)

Program Area	Informal/Foundational (Siloed)	Standardized (Collaborative)	Managed/Monitored (Informed)	Sustained/Optimized (Integrated)
Applicable Requirements		<ul style="list-style-type: none"> Responsibility for ICOR requirements resides with ICOR or ERM Program leads based on their capabilities (G) Liaisons to management and governing bodies (e.g., SAT) established within major business units (G) Duplicative tools begin to consolidate and programs rely more consistently on a standardized tool (or suite of tools) for the same functions to enable consistent reporting and performance of assessments (T) Some off-the-shelf tools used for problem solving and reporting (e.g., SharePoint) (T) 	<p>management reporting and support decision-making (T)</p> <ul style="list-style-type: none"> Analytics and visualization platforms (e.g., R, Python, Tableau) in place and configured for recurring assessment and review of data to identify anomalies and potential reporting errors (T) Off-the-shelf tools are customized and expanded to support additional aspects of internal control lifecycles and data is shared across modules/tools (T) 	



Table 2. DON Integrated Risk Management Maturity Model
 Key: People (P), Processes (Pr), Governance (G), Technology (T)

Program Area	Informal/Foundational (Siloed)	Standardized (Collaborative)	Managed/Monitored (Informed)	Sustained/Optimized (Integrated)
Applicable Requirements Integration Points OMB Circular No. A-123 (Overall) OMB Circular No. A-11, Sec. 240.27, 260.27	<ul style="list-style-type: none"> FM&C facilitates preparation of the SOA based on individual BSO and MAU certifications; no clear consideration of DON Risk Profile (Pr) 	<ul style="list-style-type: none"> “Tone at the top” is established by DON senior leadership through formal, periodic messaging about the importance of DON ERM and Internal Control Programs to the mission (P) Preparation of SOA with Risk Profile input from OCMO (Pr) ICOR assessments leverage results of program/operation reviews (e.g., system controls assessed ICOR for a system that is used to produce a key management report) (Pr) 	<ul style="list-style-type: none"> “Tone at the top” extends beyond formal messaging to day-to-day activities and is cascaded further by mid-level management (P) Internal control assessment teams are comprised of personnel that, together, understand financial and operational aspects of the DON’s business operations and assessment objectives (P) Internal Controls scoping and planning consider the Risk Profile and whether any enterprise risks might influence the scope or extent of internal control testing (Pr) Scope of the DON’s fraud risk assessment is informed by risk profile; results of ICOR assessments help the DON determine residual risk for its inventory of fraud risks (Pr) Internal control assessment results (i.e., MW) are shared with representatives to ERM Program to consider for the DON risk profile (Pr) ELC assessment reflects effective risk assessment and response processes; identifies potential program gaps in achieving ELC objectives (Pr) 	<ul style="list-style-type: none"> “Tone at the Top” is mirrored and embraced at all levels of the Department; internal controls and risk management are part of daily operations and understood as valuable to the mission (P) Preparation of the SOA is a coordinated effort between Internal Control and ERM Program leaders (i.e., SOA is based not only on individual MAU/BSO certifications, but the collective ERM and internal control assessment results reported by OCMO and FM&C) (Pr) Senior-most governing and decision-making bodies use risk and internal control information, alongside other operational performance data, to make risk-based management decisions on investment of Department resources to risk and remediation activities (G) eGRC tools integrate disparate risk/compliance management initiatives and help automate risk and internal control activities across the Department (T)



Appendix B. References

SECNAVINST 5200.35G, "Department of the Navy Managers' Internal Control Program," March 29, 2019

DoD 7000.14-R, Volume 1, "Department of Defense Financial Management Regulation (FMR)," current edition

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013

Office of the Under Secretary of Defense (Comptroller), Department of Defense, "Digital Accountability and Transparency Act of 2014 Data Quality Plan", February 8, 2019

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, "Financial Improvement and Audit Readiness (FIAR) Guidance," current edition

Government Accountability Office 14-704G, "Standards for Internal Control in the Federal Government" (also known as the "Green Book"), September 10, 2014

Office of Management and Budget Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control", July 15, 2016

- Appendix A: "Management of Reporting and Data Integrity Risk", June 6, 2018
- Appendix B: "Improving the Management of Government Charge Card Programs", January 15, 2009
- Appendix C: "Requirements for Payment Integrity Improvement", June 26, 2018
- Appendix D: Compliance with the Federal Financial Management Improvement Act of 1996", September 20, 2013

Office of Management and Budget Circular No. A-11, "Preparation, Submission and Execution of the Budget," June 29, 2018

Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Enterprise Risk Management – Integrating with Strategy and Performance (2017)



Appendix C. Acronyms

Acronym	Description
ADA	Anti-Deficiency Act
ASN	Assistant Secretary of the Navy
AU	Assessable Unit
B2R	Budget to Report
BES	Budget Estimate Submission
BOMC	Business Operations Management Council
BOP	Business Operations Plan
BSO	Budget Submitting Office
BUD	Budget Execution - Budgeting
CAP	Corrective Action Plan
CFO	Chief Financial Officer
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CONOPS	Concept of Operations
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DATA	Digital Accountability and Transparency Act
DPG	Defense Planning Guidance
DoD	Department of Defense
DoDI	Department of Defense Instruction
DON	Department of the Navy
DTT	Deficiency Tracking Tool
eGRC	Enterprise Governance Risk and Compliance
EI&E	Energy, Installations and Environment
ELC	Entity Level Control
ERM	Enterprise Risk Management
E2E	End-to-End
FFMIA	Federal Financial Management Improvement Act
FIAR	Financial Improvement and Audit Readiness
FM&C	Financial Management and Comptroller
FMFIA	Federal Managers' Financial Integrity Act
FMO	Office of Financial Operations
FMR	Financial Management Regulation
FRDAA	Fraud Reduction and Data Analytics Act
FY	Fiscal Year
G	Governance
GAO	Government Accountability Office
GPRA	Government Performance and Results Act
HQMC	Headquarters Marine Corps
ICO	Internal Controls Over Operations
ICOFR	Internal Controls Over Financial Reporting
ICOFS	Internal Controls Over Financial Systems
ICOR	Internal Controls Over Reporting
IPERIA	Improper Payments Elimination And Recovery Improvement Act Of 2012
IRM	Integrated Risk Management
ITGC	Information Technology General Controls
M&RA	Manpower and Reserve Affairs
MAU	Major Assessable Unit



Acronym	Description
MICP	Managers' Internal Control Program
MW	Material Weakness
NAVAUDSVC	Naval Audit Service
NAVINGEN	Naval Inspector General
NDS	National Defense Strategy
NMS	National Military Strategy
NSS	National Security Strategy
OASN	Office of Assistant Secretary of the Navy
OCMO	Office of the Chief Management Officer
OGC	Office of General Counsel
OMB	Office of Management and Budget
OPNAV	Office of Chief of Naval Operations
OSD	Office of the Secretary of Defense
P	People
P2P	Performance to Plan
POM	Program Objectives Memorandum
PPBE	Planning, Programming, Budgeting, and Execution
Pr	Processes
RD&A	Research Development and Acquisition
SAT	Senior Assessment Team
SD	Significant Deficiencies
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SMC	Senior Management Council
SOA	Statement Of Assurance
Sub-AU	Sub-Assessable Unit
T	Technology
UNSECNAV	Under Secretary of the Navy

